

Alerta de seguridad informática	8FFR-00120-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Noviembre de 2019
Última revisión	23 de Noviembre de 2019

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de fraude no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado fraude, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cuatro portales bancarios fraudulentos asociados a una IP que suplantan el sitio web oficial de **Banco de Chile**, lo que podría servir para el robo de credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Indicadores de Compromisos

URL's

URL Sitio Clonado:

https://new[.]29studios[.]com/wp-content/plugins/duplicator/lib/nuevo/servicios[.]aumento[.]bancochile[.]cl/qzu3tv15qv/7jii1_persona/login_irg2/index/loggingj3n/

https://new[.]29studios[.]com/wp-content/plugins/duplicator/lib/nuevo/servicios[.]aumento[.]bancochile[.]cl/m2h5ozejie/53b8l_persona/login_jj5u/index/loginheya/

https://new[.]29studios[.]com/wp-content/plugins/duplicator/lib/nuevo/servicios[.]aumento[.]bancochile[.]cl/d22qpe9aas/gppz2_persona/login_yo34/index/loginjx0x/

https://new[.]29studios[.]com/wp-content/plugins/duplicator/lib/nuevo/servicios[.]aumento[.]bancochile[.]cl/5wvt6vamfe/sxn4b_persona/login_upkz/index/loginfp17/





Domain 29studios.com ⓘ			
29studios / com /  Subdomains			
record type	TTL	value	
A	300	93.113.110.46	
NS	300	ns1.nimbushosting.co.uk	 Zones on DNS server 45.32.239.22
NS	300	ns2.nimbushosting.co.uk	 Zones on DNS server 94.126.44.133
NS	300	ns3.nimbushosting.co.uk	 Zones on DNS server 5.254.66.139
MX	300	1 aspmx.l.google.com	
MX	300	5 alt2.aspmx.l.google.com	
MX	300	5 alt1.aspmx.l.google.com	
MX	300	10 alt4.aspmx.l.google.com	173.194.202.27
MX	300	10 alt3.aspmx.l.google.com	108.177.97.27
TXT	300	v=spf1 include:_spf.google.com ip4:93.113.110.46 ip4:176.56.62.239 ~all	
SOA	300	Mname	ns1.nimbushosting.co.uk
		Rname	hostmaster.nimbushosting.co.uk
		Serial number	2018041302
		Refresh	3600
		Retry	3600
		Expire	86400
		Minimum TTL	3600

Ilustración 1 Dominio donde se Aloja Url del Banco de Chile, Falso y DNS que utiliza

Certificados

		Criteria	Identity = '29studios.com'		
Certificates	crt.sh ID	Logged At	Not Before	Not After	Issuer Name
		2005422919	2019-10-16	2019-10-16	2020-01-14
	2005422166	2019-10-16	2019-10-16	2020-01-14	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1923929437	2019-09-23	2019-09-23	2019-12-22	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1916406036	2019-09-23	2019-09-23	2019-12-22	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1830923974	2019-08-17	2019-08-17	2019-11-15	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1780664746	2019-08-17	2019-08-17	2019-11-15	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1709036807	2019-07-24	2019-07-24	2019-10-22	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1703752780	2019-07-24	2019-07-24	2019-10-22	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1615514324	2019-06-18	2019-06-18	2019-09-16	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1588662854	2019-06-18	2019-06-18	2019-09-16	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1514657752	2019-05-25	2019-05-25	2019-08-23	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1508725109	2019-05-25	2019-05-25	2019-08-23	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1399483902	2019-04-19	2019-04-18	2019-07-17	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1399443785	2019-04-19	2019-04-18	2019-07-17	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1325066558	2019-03-26	2019-03-26	2019-06-24	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1317608725	2019-03-26	2019-03-26	2019-06-24	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1212069835	2019-02-17	2019-02-17	2019-05-18	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1212070219	2019-02-17	2019-02-17	2019-05-18	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1141389006	2019-01-24	2019-01-24	2019-04-24	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1141386994	2019-01-24	2019-01-24	2019-04-24	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1043011036	2018-12-19	2018-12-19	2019-03-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	1043005563	2018-12-19	2018-12-19	2019-03-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	975991392	2018-11-25	2018-11-25	2019-02-23	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	975990851	2018-11-25	2018-11-25	2019-02-23	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	877935008	2018-10-20	2018-10-20	2019-01-18	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	877945310	2018-10-20	2018-10-20	2019-01-18	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	823425576	2018-09-26	2018-09-26	2018-12-25	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	788654170	2018-09-26	2018-09-26	2018-12-25	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	789581150	2018-08-21	2018-08-21	2018-11-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	686201753	2018-08-21	2018-08-21	2018-11-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	670755192	2018-07-28	2018-07-28	2018-10-26	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	649288850	2018-07-28	2018-07-28	2018-10-26	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	568396692	2018-06-22	2018-06-22	2018-09-20	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	544071818	2018-06-22	2018-06-22	2018-09-20	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	491095501	2018-05-28	2018-05-28	2018-08-26	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco de Chile

IP

93.113.110.46




Domain 29studios.com is located on IP address << 93.113.110.46 >>	
Block start	93.113.110.0
End of block	93.113.110.255
Block size	256  Domains in block
Block name	NIMBUS-VPS-14
AS number	<u>21396 31708</u>
Parent block	<u>93.113.110.0 - 93.113.111.255</u>
Organization	<u>Nimbus Hosting Ltd.</u>
City	<u>Leatherhead</u>
Region/State	England
Country	 GB , United Kingdom
Host name	29studios-com02.nh-serv.co.uk
Domains	1  29studios.com

Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco de Chile

Localización

Leatherhead, England, Reino Unido

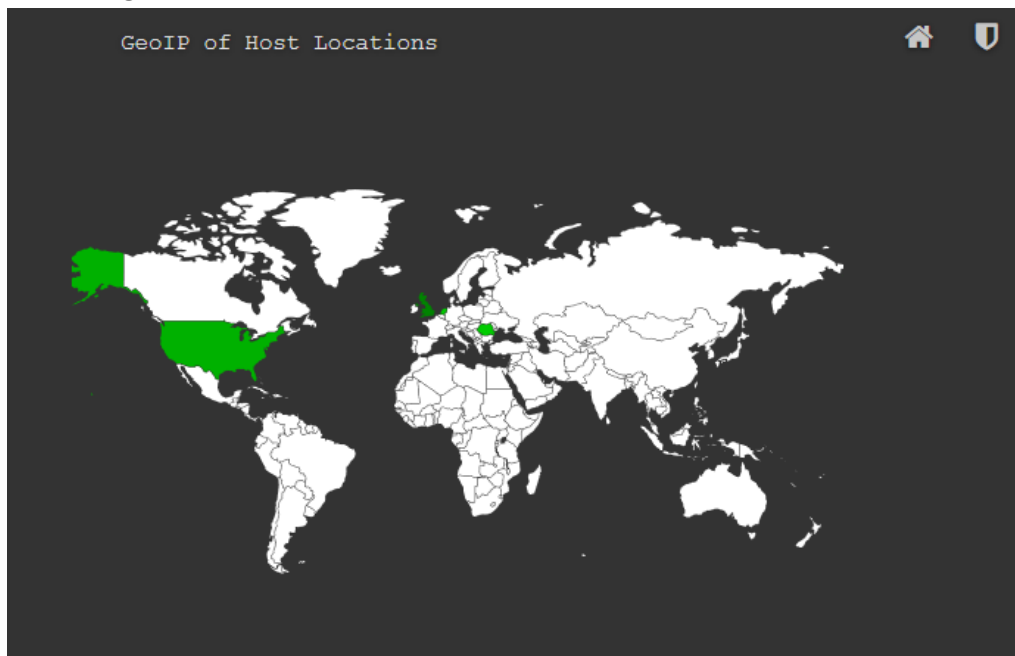
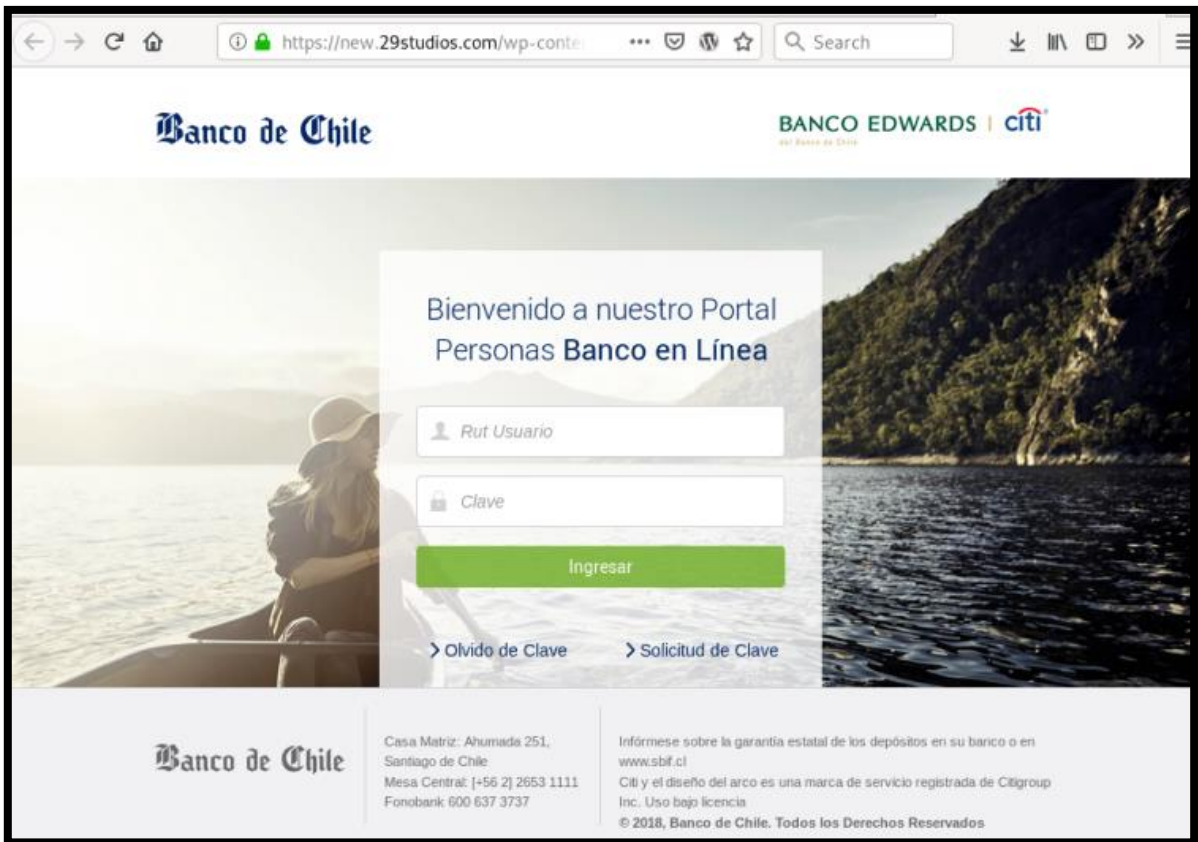


Imagen del sitio



Whois

```
Domain Name: 29STUDIOS.COM
Registry Domain ID: 1544120862_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2019-02-25T09:42:46
Creation Date: 2009-02-24T21:20:03
Registrar Registration Expiration Date: 2020-02-24T21:20:03
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Reseller: Nimbus Hosting
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Essex
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: GB
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext:
Registrant Email: https://tieredaccess.com/contact/5e0ebb1d-df16-44eb-bafb-b38e12134285
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext:
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext:
Admin Email: REDACTED FOR PRIVACY
Registry Tech ID:
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext:
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext:
Tech Email: REDACTED FOR PRIVACY
Name Server: ns1.nimbushosting.co.uk
Name Server: ns2.nimbushosting.co.uk
Name Server: ns3.nimbushosting.co.uk
DNSSEC: unsigned
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-02-25T09:42:46 <<<
```

Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre su existencia, para evitar que se conviertan en víctimas del fraude.
- Ser precavidos frente a este tipo de páginas fraudulentas.
- Bloquear en los proxy o sistemas de control de contenido, hacia la URL maliciosa
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing